FINAL REPORT

CONTROL OF UNCLASSIFIED TECHNOLOGY WITH MILITARY APPLICATION

15 APRIL 1983

Contract No. MDA903-83-C-0055

Submitted to:

Director for Counterintelligence and Security Policy
ODUSD(P), Pentagon 3C290
Washington, D.C. 20301

Submitted by:

Advanced Technology Systems, Inc.
8027 Leesburg Pike, Suite 701A
Vienna, VA 22180

Approved For Release 2009/01/21 : CIA-RDP87B01034R000400060001-8

II. EXECUTIVE SUMMARY

BACKGROUND

Valuable U.S. unclassified technology with military application is leaving our shores and is providing our adversaries with the means to increase their military potential to the detriment of U.S. national security interests. The U.S. intelligence community has concluded that if this situation is allowed to continue, the military posture of our adversaries will improve at an accelerated pace and reduce U.S. lead time advantage in certain important areas of research and development. Notwithstanding these warnings, the U.S. Government has not taken the initiative to deny our adversaries that which they need to cut their production costs, shorten their production times, and improve the quality of military products that may someday be used against this nation.

Over the years, efforts to control or restrict the dissemination of unclassified technology with military application has met with resistance from various quarters of the government, industry, and the scientific community. Moreover, Congress has continued to press for legislation that would encourage public disclosure, the most obvious example being the enactment of the Freedom of Information Act. This legislation, in particular, tended to create an attitude within the government to push scientific and technical data into the public domain. Indeed, the theme of "openness in government," established in law, is carried through a wide variety of DOD issuances that establish mechanisms through which technology may be transferred.

Though the DOD shares the view that we cannot totally stop our adversaries from acquiring the military-related technology in a free society and that stemming the flow of such technology is, in itself — complex, the Deputy Under Secretary of Defense (Policy) directed that a report be developed to formulate recommended actions that could be taken unilaterally by the Department to bring about more effective control over important military technology.

OBJECTIVES

The objectives of this effort are: 1) to develop methods designed to give effect to control of U.S. militarily-significant technology within DOD and defense industry, given the parameters of U.S. laws and implementing regulations; 2) to focus attention on principal mechanisms through which unclassified technology with military application is transferred; and 3) to identify any weakness in these mechanisms and propose a methodology to identify technologies to be protected.

CURRENT CONTROLS AUTHORIZED

U.S. Laws

Statutory limitations governing the control of unclassified technology with military application, are found in the Mutual Security Act of 1954, as amended, the Arms Export Control Act of 1976 and the Export Administration Act of 1979. These laws govern the export of goods, services, and related technical data from the U.S. as well as the access of foreign nationals to such items in the U.S.

From these laws and their implementing issuances, it is clear that the President has authority to control the export of unclassified technology. Further, we believe, that through Presidential delegations, the Secretary of Defense has a mandate to fully implement the provisions of the export control laws as their provisions govern information owned by, produced by or for, or under the control of the DOD. Moreover, we are of the view that it is a prerogative of the Secretary of Defense to interpret the laws and implementing regulations as they pertain to this body of material. Therefore, it would appear that actions taken by the Secretary of Defense to control unclassified technology with military application in both the DOD and Defense industries would be consistent with the letter and intent of applicable law.

For controlling this valuable technology, however, the provisions of existing U.S. laws appear to work at cross purposes. For example, if unclassified technical data that is related to items on the Munitions Control List were in government records and such records were requested by a member of the public under the Freedom of Information Act (FOIA), there is no basis in law to withhold the data. Once the release is made, control of the technical data is lost and it would appear that under the provisions of the export control laws and implementing regulations, the requester could export the data without benefit of license.

A proposed protective exemption allowing government agencies to withhold "technical data" that may not be exported without an approval or license has been recommended by this Administration to amend the FOIA. Historically, Congress has been reluctant to amend the FOIA by adding more exemptions. However, Congress may not be so hesitant in amending the export control laws to make it explicit that information subject to such laws may be withheld from public disclosure under the (b)3 exemption of the FOIA on the basis of their finding that public disclosure of information subject to such laws is tantamount to export.

DOD has also developed a proposal to amend title 10, United States Code, to provide authority to the Secretary of Defense to regulate the dissemination of information the disclosure of which outside the Government could reasonably be expected to result in the loss of a significant military technological or operational advantage to the U.S. If such legislation were enacted, such information could be withheld from requestors under the (b)3 exemption ("withholding statute") of the FOIA.

Legislative Recommendations to Alter Current Contro[redacted] Authorized

We support these DOD efforts to exempt from public disclosure unclassified technology with military application and recommend that DOD continue to urge corrective legislation that could take the form of either:

- An amendment to the FOIA itself;
- An amendment to the Export Administration Act and the Arms Export Control Act; or
- By separate legislation that would become withholding statutes under section (b)3 of the FOIA.

Presidential Directive

If legislative initiatives are unsuccessful, consideration might be given to expanding the use of the classification system to protect the technical data of concern.

A Presidential Order has already been promulgated that provides the proper classification of information and its safeguarding against unauthorized disclosure. Indeed, a substantial number of people in both government and industry have expressed the view that militarily-significant technology could only be protected against public disclosure and foreign dissemination by use of the classification system.

A proposal was developed by the DOD to introduce a fourth level of classification, "Restricted" to be applied to information, the unauthorized disclosure of which reasonably could be expected to cause the loss to the U.S. of a technological or military advantage and thus require protection in the interest of national security. As an alternative to the "Restricted" proposal, DOD also has under consideration a concept for the application of the Confidential classification to this body of material with modification of the safeguarding requirements that would permit less restrictive access and handling. The advantage in using a security classification to protect militarily-significant technology is that such information classified as either "Restricted" or Confidential may be withheld from requestors under the FOIA. The disadvantages would be that classification of this body of information would not be cost effective and would impede U.S. research, development and foreign marketing operations to an unacceptable degree.

If it becomes necessary to resort to classification as a means to control this body of material it might best be achieved by:

- Creating a fourth level of classification with reduced handling requirements; or by
- Using the Confidential classification with similarly reduced safeguarding requirements.

Departmental Issuances

It has been a long-standing policy of the DOD to maximize, consistent with interests of national security, the amount of information provided to the American people about DOD operations and activities. This theme is carried through most DOD Directives and Instructions that establish mechanisms through which unclassified technology with military application is transferred to foreign entities. Generally, provision is made throughout these issuances to protect classified information against unauthorized disclosure that may be subject to transfer through the mechanism established by the Directive or Instruction. However, little attention focused on the need to control unclassified technology with military application, whether or not it is related to classified information, that may be transferred through such mechanisms. Further, very few of the issuances permitting or requiring release to the public invite attention to the export restrictions under law that are applicable to the information processed through such mechanisms.

In most cases, the DOD issuances reviewed also do not make it explicit whether they apply to industry. Nevertheless, for most programs established by these issuances, defense industry is perhaps the principal developer of, and primary repository for, unclassified technology with military application.

Though the "openness" theme is a commendable one in our society, with certain knowledge that the Soviets and others are acquiring U.S. technology to their advantage and to the detriment of U.S. national security interests, each of the DOD issuances permitting or requiring release of information to the public needs modification to ensure that unclassified technology with significant military application is denied our adversaries.

Recommendations

Accordingly, we recommend that:

- The Secretary of Defense cause the immediate review of the DOD Directives and Instructions that permit or require the release of information to the public for purposes of providing for the protection of unclassified technology with military application;
- As an interim measure, the Secretary of Defense should establish criteria for identification of those military technologies considered significant, and should direct DOD components to take appropriate actions to ensure that technologies that meet such criteria are not disseminated to the public or otherwise provided to foreign nationals.

PRINCIPAL MECHANISMS THROUGH WHICH TECHNOLOGY IS TRANSFERRED

Discussion

There is a wide variety of mechanisms through which unclassified technology with military application is transferred both legally and

illegally. For purposes of this report, they are consolidated into six general categories; public release, clandestine, sales, exchange agreements, meetings, and international corporate arrangements. Each is treated in detail in the main body of this report.

We find that within each mechanism, adequate provisions is made for the protection of classified technological information against unauthorized disclosure and that foreign access to this body of information is controlled effectively under the National Disclosure Policy. However, as pointed out above, the issuances governing these mechanisms generally fail to provide for the protection of unclassified technology with military application against public disclosure and foreign access. Thus, important technical data is easily acquired by our adversaries through a number of channels. We also find that personnel in both DOD and its contractor facilities who process information through these varied mechanisms are uncertain as to what technical data needs protection against disclosure because of a paucity of top level guidance. For example, they view the Militarily Critical Technologies List (MCTL) as vague in its application. The MCTL is not a control list per se nor does it preclude public disclosure of the items listed.

For information generated within or processed through the mechanisms in place in DOD and industry for the dissemination of technology, there is no standard that is uniformly applied to each such mechanism to protect unclassified technology with military application against public disclosure and foreign access.

Recommendations

To provide for more effective control over unclassified technology with military application that is processed through such transfer mechanisms, we have recommended specific actions that, if adopted, would:

- define critical technology and establish criteria for identifying such technology;
- apply such definition and criteria uniformly to all mechanisms through which technology is disseminated; and
- establish guidance for the use of all DOD personnel and contractors that would form the basis for determinations relative to public release approval, export license applications, patent applications and disclosures at symposia, seminars and other public meetings.

METHODOLOGY IN IDENTIFYING ELEMENTS OF INFORMATION THAT REQUIRE CONTROL

Discussion

In-depth discussions were held with over two hundred people in government and in industry who are directly involved in operations that deal with the handling of unclassified technology with military application. Though these people expressed different views on how this important information should be controlled, there is a consensus among

them that the government has an obligation to identify with more precision what needs to be controlled.

An unclassified April 1982 CIA report, "Soviet Acquisition of Western Technology," describes the Soviet program to acquire U.S. and Western technology and projects Soviet priority technological needs for such technology through the 1980's that could someday find application in weapons used to threaten the West. We found that the CIA report is favorably accepted throughout the Executive and Legislative Branches and because it is unclassified, it may be generally circulated. Notwithstanding its obvious usefulness in focusing attention on the technology transfer problem and lending guidance as to what to protect against, little has been accomplished in the way of utilizing the report in such a manner. In our view, this report appears to be a logical place for DOD to begin to set its priorities for the control of unclassified technology with military application. The projected Soviet technological needs and acquisition targets through the 1980's, identified in the CIA report, are nearly all defense-related technologies. It is reasonable to assume that certain elements of information comprising the technologies are classified and are adequately safeguarded against unauthorized disclosure. There is a substantial amount of information, however, related to these technologies which, though unclassified, will assist our adversaries to an immeasurable degree to acquire the total technology if these elements of information continue to be uncontrolled. It is this information that needs to be identified.

We believe that the task can be accomplished in a manner similar to that used by DOD to identify for each classified program, project, and system the items of information within these programs that are classified. Under this procedure, program, project or systems managers, in accordance with DOD guidance, identify items of information within their respective areas that are determined to require classification.

In the case of unclassified technology with military application, the approach would be to develop statements for each technology or equipment identified by the intelligence community as Soviet priority targets, identifying unclassified aspects of such technology or equipment that should be protected against public disclosure and foreign dissemination. We do not contemplate the development of another Militarily Critical Technologies List in different form. Instead, we propose the preparation of a statement for each technology already identified as a Soviet high priority target that would serve as an advisory as to what there is about that technology that is important for an adversary to learn to lead him to its acquisition.

The preparation of such guidance statements may appear to some to be a formidable task. However, to the many engineers, research and development people and others from whom we solicited views on this subject, the accomplishment of the task in considered feasible, practical and not as complex as some would believe.

This task could be accomplished by forming small task groups for each technology identified, comprised of knowledgeable representatives of the research and engineering staffs of the Secretary of Defense and affected military departments and representatives of DIA, or other appropriate intelligence components. These teams would be charged to prepare a guidance statement on each technology to include information that is determined to be unclassified but nevertheless militarily-significant in the sense that it is not possessed by, or available to, potential adversaries and which, if acquired by them, would permit a substantial advance in their military capabilities or lead them to acquisition of the technology of concern. For each technology, the team should be isolating that body of unclassified information that satisfies one or more of the following criteria:

- it contributes to the superior characteristics (performance, reliability, maintainability or cost) of current military systems;
- it relates to specific military deficiencies of a potential adversary and would contribute significantly to the enhancement of their military mission;
- it concerns an emerging technology with high potential for having a major impact upon advanced weapons systems. Such statements should be reviewed on, at least, an annual basis and changed as new information is developed.

The guidance statements should be widely disseminated to DOD systems, projects and program managers, Defense contractors involved in covered subject areas, public affairs officers, and export and patent application case processors. These statements should also be passed to the Office of Munitions Control of the Department of State and the Office of Export Administration of the Department of Commerce together with a request that these offices, in turn, caution the commercial sector and seek their cooperation in controlling such information.

These guidance statements would provide the basis for precise identification of unclassified data elements of information related to Defense programs, projects or systems, whether classified or unclassified, that in any way involve the technology to which the guidance pertains. Once the data elements are identified by DOD program, project, or systems managers, that identification needs to be conveyed to those who generate, acquire or access the information in government and industry together with instructions relative to control and disclosure.

Recommendations

We recommend that:

- DOD establish priorities as to what unclassified technology with military application needs to be protected with the focus of the effort centered on the technologies already identified by the U.S. intelligence community as Soviet priority targets.

- Task groups be formed for purposes of developing a guidance statement relative to each such technology.
- The guidance statements be used to satisfy the Secretary's statutory responsibilities to specify what unclassified "technical data" is subject to export licensing requirements.
- The guidance statements be widely disseminated for use of license and patent application case processors, public affairs officers and more particularly, to DOD program, project, and systems managers to identify data elements of information within each such activity under their jurisdiction that require control.
- Disclosure decisions be based on such guidance and the published definition and criteria for critical technology.

METHODOLOGY FOR NOTIFYING INDUSTRY OF ITEMS IDENTIFIED AS REQUIRING CONTROL

Discussion

Much of the information that is addressed in this report is generated, acquired, or otherwise handled through DOD contractual arrangements with industry. It is through such contractual arrangements that the DOD can identify to industry that information determined by the DOD to require protection against public disclosure and foreign dissemination.

A contract specification form could be used as an instrument to identify for industry elements of unclassified information that are militarily-significant technology and are required to be approved for public release by the DOD or are required to have export license prior to foreign dissemination. This instrument could be made part of the contract and would obligate industry to protect the information identified therein as DOD desires that it be protected.

Recommendation

We recommend that Defense Acquisition Regulations prescribe that unclassified technology with military application requiring protection against public disclosure and foreign access be identified in the contract (classified or unclassified) by means of such a contract specification.

ALTERNATE METHODS OF CONTROL

Discussion

There are four methods of controlling unclassified technology with military application that we believe are worthy of consideration. The first is control by classification.

- A substantial number of people in both government and industry have expressed the view that unclassified technology with military application cannot be protected unless it is classified. The existing three-tier classification system has not been effective in protecting this body of information. The basic reason is that information related to this technology has not, standing alone, appeared to meet the damage criteria established by the applicable Executive Order. Also, classification of currently unclassified technology with military application even at the lowest level now prescribed in the security classification system would require the imposition of safeguarding requirements that would be unacceptable to many. Those who previously had free access to this information for research and development, and marketing operations both foreign and domestic, would be impacted adversely.
- In recognizing these concerns, the DOD considered introduction of a fourth level of classification with a lower threshold than the current damage criteria. If this proposal was adopted, then information that could be identified as critical technology could be classified and protected adequately against unauthorized disclosure. The safeguarding requirements associated with this fourth level of classification would be different and less stringent than those now in force for information classified at the Confidential level. An alternative concept under consideration by DOD would be the use of the Confidential classification with similarly less restrictive safeguarding requirements. Either way, the information of concern would be classified pursuant to an Executive Order and exempt from mandatory disclosure under the FOIA.

Secondly, control of unclassified technology with military application in industry and the DOD could be effectuated by the imposition of standard safeguarding requirements that, though less stringent than those prescribed for classified information, may suffice to protect this information against public disclosure and foreign dissemination. Such requirements would be imposed on industry through contracts or other legally binding documents and would be made applicable to DOD by regulatory issuances. These safeguarding requirements would not preclude the public disclosure of information under the FOIA. Nevertheless, their application would have the effect of stemming the initial flow of the information into the public domain.

As with classification, these requirements would involve some costs to both government and industry, and may result in impeding the flow of information between U.S. entities.

A third method of control of unclassified technology with military application would involve a contractual arrangement or agreement between the DOD and the defense contractor whereby the contractor would be obligated to protect such information by the implementation of self imposed controls. The contractor would be advised that unclassified

technology with military application identified in the contract specification is "Technical Data" as that term is used in the export control laws and regulations. The contractor would also be notified that such information shall not be disclosed publicly nor accessed by foreign nationals without specific authorization of the contracting activity or by export license. The contractor would be obligated to protect the information accordingly. Violation of these requirements would be tantamount to violation of the export control laws and could constitute a violation of the contract itself. The Defense Investigative Service, for classified contracts, and the Defense Contract Audit Agency for unclassified contracts, would oversee implementation. This proposed method of control would be favored by industry in that the procedural requirements for effective implementation are left to their discretion. However, the "controlled" information still remains subject to disclosure under the FOIA.

The fourth method would be to protect the information in industry as proprietary data is protected.

- Defense contractor representatives gave a clear indication that there is no standard method nor are there established sets or rules applicable to the protection of proprietary data against public disclosure. Notwithstanding this lack of uniformity, it is generally viewed in industry that the methods used to protect proprietary data satisfy corporate interests.
- It would not appear prudent for the Government to accept a company's assurance that it will protect "technical data" as "proprietary data" without certain knowledge of the adequacy of the limitations applied. The most serious flaw in this method is that without any additional constraints, industry would be free to disseminate the information identified by government as they are now free to disseminate that which is proprietary to the company. This could include disclosure in foreign sales and marketing when it was in the interest of the contractor.

Recommendations

Concerning these methods of control, we recommend the third alternative cited above be adopted, and that:

- The Defense Acquisition Regulations should be amended to require that every contract (classified or unclassified) involving unclassified technology with military application identified as requiring protection must contain a provision that the contractor shall not disclose such information to the public, or otherwise permit access by foreign nationals without specific authorization of the contracting authority or as may be permitted pursuant to an export license, and that the contractor agrees to adopt measures to protect this information accordingly.

- The Defense Investigative Service and the Defense Contract Audit Agency should be directed to monitor compliance.
- An extensive education and awareness program be undertaken immediately that is designed to convey the requirements of these initiatives to DOD employees engaged in export license cases, patent application cases, public affairs review and to contractors performing in affected programs.

SUMMATION

There has been and continues to be a significant loss of valuable U.S. unclassified technology with military application that is easily acquired by our adversaries, thus providing them with the means to increase their military potential to the detriment of U.S. national security interests. In our open society, it is neither feasible nor desirable to control totally this body of important information. Consequently, we must set our priorities and protect that which we possess in ways that are both practical and appropriate.

A coherent U.S. program to control the loss of unclassified technology with military application must be established. First, the laws that impact on the control of this valuable data must be amended to make them compatible rather than working at cross purposes, e.g., the export control laws vs. the Freedom of Information Act. Next, Government must identify that information that is determined to require protection against public disclosure and foreign access with a greater degree of precision.

Within the DOD and among its contractors, mechanisms need to be established to ensure that uniform and comprehensive controls are imposed over the information in question. In this connection, it should be noted that whatever system of controls is implemented, it is likely to be ineffectual without full cooperation of both government and industry.

The Department of Defense, working within the parameters of existing laws and implementing regulations, is obligated to define what unclassified technology with military application requires control and to set forth criteria to assist DOD officials and defense contractors to identify the information deserving protection. Such definition and criteria should be applied uniformly and comprehensively to all mechanisms through which technology is transferred. There is a particular need for guidance at the lower echelons of command and supervision on which to base determinations relative to what can be said publicly about a particular technology.

Finally, the responsibilities for effective implementation of this program must be vested in one controlling OSD office.

VI. CONCLUSIONS

A. The loss of unclassified technical data that is related to technologies with significant military application is a serious national security problem.

1. There is a consensus in government and industry that the Soviet Union has benefited substantially from its acquisition of Western technology with military application, and that its efforts are unlikely to abate in the 1980's.

2. Soviet successes in acquiring this valuable data have enabled them to build higher quality weapons systems at lower costs and in a shorter period than would otherwise have been the case.

3. Soviet acquisition of Western technology has also enabled them to build countermeasures to U.S. systems in a more rapid and effective manner than would otherwise have been the case.

4. The technological advantages historically enjoyed by the United States has been eroded by the Soviets' collection and utilization of Western technology thereby causing the U.S. to spend more on its military programs.

B. Total control of unclassified technology with military application in our open society is neither feasible nor desirable.

1. Governmental restrictions upon private enterprise with respect to the development of such technology using its own resources are contrary to the system of free enterprise, and may actually work to the disadvantage of U.S. national security interests by frustrating industrial initiative and cooperation. While the government might encourage voluntary restraint on the part of private industry in developing or selling technology of obvious and significant military application, government efforts to restrict such activities should not extend beyond the export control laws.

2. For work being performed pursuant to government contract, however, the government has the right, if not the responsibility, to ensure that the benefits of technology developed under its sponsorship are retained by the United States for as long as possible. This implies limits on what may be disclosed to the public as well as what may be exported to or accessed by other countries or their representatives.

C. A coherent program to control the loss of unclassified technology with military application produced pursuant to government contract does not exist.

1. Export control laws do not adequately control unclassified technical data related to technologies with military application, nor is there an effective means of otherwise controlling its public disclosure and foreign access.

2. Existing export control regulations leave open to broad interpretation what technical data is subject to export licensing requirements.

3. Existing export control regulations, though recognizing that public disclosure is tantamount to export by exempting from a specific export license requirement that which is released to the public, do not in any way restrict domestic dissemination of technical data subject to export licensing requirements.

4. The Freedom of Information Act does not exempt technical data that is subject to export controls from release to the public. Insofor as DOD is concerned, this has resulted in such data, as a general matter, being affirmatively pushed into the public domain through a number of mechanisms without regard for whether it may be subject to export control laws and regulations.

5. Internal DOD policies governing the control of unclassified technical data with military application are inadequate not only in terms of their failure to recognize and restrict public dissemination of and foreign access to technical data subject to export controls, but also because these policies are not, in all cases, made applicable to industry by contract or other legally-binding document.

D. The key ingredients in establishing a coherent system of control are the identification of what technical data with military application requires protection against public disclosure and foreign access, and the establishment of priorities for such protection.

1. Under existing statutes, the Secretary of Defense is given broad authority both to recommend changes to U.S. export control lists, and to control the export and dissemination of defense goods, services, and related information within DOD and defense industry. These authorities place him in a unique position to prescribe what "technical data" shall be subject to export and dissemination controls, and to establish priorities for the protection of information so identified.

2. The U.S. intelligence community has provided a basis upon which such determinations could be made, but DOD has not yet set its priorities for nor identified with any precision that technical data that should be protected in either the export control process or by means of other dissemination controls. The Militarily Critical Technologies List produced by DOD pursuant to a requirement of the Export Administration Act of 1979 has not served these purposes.

3. Both government and industry people who handle unclassified technology with military application on a frequent basis lack sufficient guidance as to what segments they should protect and in what order. They strongly urge the development of such guidance.

E. The varied mechanisms in place in both the DOD and among its contractors, through which unclassified technology with military application is transferred, are deficient in the sense that they fail to ensure control over the information in question.

1. Current DOD policies and procedures governing the public disclosure of, and foreign access to unclassified technology with military application do not provide sufficiently comprehensive protection against the loss of such information through the variety of mechanisms discussed in Part V, Section B, of this report.

2. Effective controls are not imposed on unclassified technical data generated, acquired, or otherwise handled by defense contractors, except insofar as such data is related to a classified contract nor are there effective and practical methods in place for the enforcement of such controls.

F. It is feasible to establish controls in DOD and defense industry to protect unclassified technology with military application from public disclosure, or access by foreign nationals without: (1) incurring substantial costs; (2) inhibiting the sharing of information within government and industry; (3) inhibiting the ability of private concerns to do business with DOD; or (4) impairing the capability of defense industry to compete successfully in both domestic and international commerce. Notwithstanding, without full cooperation of both government and industry, the implementation of any system of controls is likely to be ineffectual.

VII. RECOMMENDATIONS

A. TO PROVIDE FOR A COHERENT SYSTEM OF CONTROL:

1. Legislation should be sought that, if enacted, would exempt technical data, subject to export control requirements, from the provisions of the Freedom of Information Act (FOIA). Such legislation could take the form of either:

a. an amendment of the FOIA itself, such as that proposed by the Administration; (See Part V, Sec. A.3.b)

b. amendments to the Arms Export Control Act of 1976 and the Export Administration Act of 1979; or

c. by separate legislation that would become "withholding statutes" under section b (3) of the FOIA. (See Part V, Sec. A.3.b and c.)

2. Though not viewed as preferable, if these legislative initiatives are unsuccessful, consideration should be given to expanding the use of the classification system to exempt such data from the provisions of the FOIA and otherwise protect it from public disclosure and foreign access. This might be achieved, as DOD attempted earlier, by creating a fourth level of classification with reduced handling requirements, or by establishing such reduced requirements for a particular category of information (e.g. technical data with military application that is required to be protected under specific criteria), classified at the CONFIDENTIAL level. (See Part V, Sec. A.6.c. and d.)

3. By directive or other appropriate policy instrument, the Secretary of Defense should define unclassified technical data that should be protected against public disclosure and foreign access and set forth criteria to assist in identifying such data.

a. This definition and criteria should be applied uniformly throughout the DOD and defense industry to form the basis for making determinations relative to, inter alia, public release approvals, export license and patent applications and disclosures at symposia, seminars and other public meetings.

b. Such issuance should prescribe that technical data defined therein should not be disclosed publicly or exported without specific authorization when it can be determined that the information:

(1) is not already possessed by, or available to potential adversaries;
(2) provides an advantage in terms of the performance, reliability, maintenance, or cost of current U. S. military systems over systems currently employed by adversaries;

(3) relates to specific known deficiencies in the capability of potential adversaries, and would contribute significantly to such capabilities; or
(4) relates to an emerging technology with high potential for having a major impact upon advanced weapons systems of the United States.

4. Pending promulgation of the issuance recommended in paragraph 3., above, the Secretary of Defense, by memorandum to heads of DOD Components, should express his concern over the loss of unclassified technology with military application, define unclassified technical data that is determined to require protection against public disclosure and foreign access, and caution against such disclosure.

B. TO IDENTIFY WHAT TECHNICAL DATA SHOULD BE PROTECTED

1. Over and above the actions recommended in paragraph 3., above (definition and criteria), the Secretary of Defense should direct that an effort be initiated immediately, using the following methodology, to identify unclassified technical data with military application that requires protection:

a. The effort should take as its starting point those technologies already identified by the intelligence community as being of military significance to, and priority targets of, the Soviet Union. (See Part V, Sec. D.4). If further refinement of this Soviet priority target list is believed required, it should be accomplished on an expeditious basis.

b. For each such technology or class of technologies, a team, consisting of knowledgeable representatives of the research and engineering staffs of the Secretary of Defense and the Military Departments and representatives of DIA, or other appropriate intelligence components, should develop within a 30 - day time frame, a guidance statement that would identify in generic terms the unclassified technical data related to each such technology that requires protection under the criteria established by the Secretary of Defense (See recommendation 3. above.). These guidance statements should also include, if the legislation mentioned under recommendation A.1, above, were enacted, a statement to the effect that technical data, so identified, may be withheld under the FOIA..

c. The guidance statements should, to the extent practicable be reviewed by, and comments solicited from, affected program, project and systems managers and engineers in the DOD, and contractor representatives expert in the particular and related fields of endeavors.

d. The guidance statements developed as a result of this process should be approved by the Under Secretary of Defense for Research and Engineering, and, once approved, given wide circulation throughout DOD and affected defense contractors. The guidance statements should be used as the basis for:

(1) satisfaction of the Secretary's statutory responsibilities to specify to the Secretaries of State and Commerce what unclassified "technical data" is subject to export licensing requirements;
(2) DOD processing of export licensing and patent application cases;
(3) the imposition of controls upon dissemination of information to the general public, or otherwise to foreign nationals.

2. Review for currency of the technologies of concern, and the guidance statements relating thereto, should be accomplished at least annually and should be subject to change at any time based on new information.

C. TO ESTABLISH MECHANISMS OF CONTROL:

1. The Secretary of Defense should direct that the Defense Acquisition Regulations be amended to require for every contract involving technical data that requires protection, as determined by the contracting activity, provisions that contain the following features:

a. The contracting activity would be obligated to describe to the contractor the technical data involved in, or pertinent to, the performance of the contract that is determined to warrant protection against public disclosure and foreign access. This description would be included in a contract specification;

b. The contractor would undertake not to disclose the information so identified to the public, or otherwise permit access by foreign nationals, without specific authorization of the contracting authority or as may be permitted pursuant to an export license;

c. The contractor would be required to establish internal procedures to implement the requirements described in b., above. The contracting activity should, to the extent practicable, determine the adequacy of such procedures prior to the award of a contract; and

d. The contractor should be placed on notice that such procedures may be subject to inspection by the Defense Investigative Service (where the firm holds a classified contract) and/or the Defense Contract Audit Agency (where the firm holds an unclassified contract), and that failure to establish and/or abide by such procedures may constitute grounds for the imposition of a range of administrative sanctions from warning notice to termination of the contract.

2. The Secretary of Defense should direct that all DOD directives and other issuances that relate to mechanisms through which technology is transferred and that are identified in the Appendix to this report, be reviewed and amended, as appropriate, to prohibit the release of technical data that is determined to warrant protection against public disclosure or foreign access without specific authorization. USD (R&E), ASD (PA), and DUSD (P) should jointly monitor this effort.

D. TO ENSURE COMPLIANCE:

1. The Secretary of Defense should designate a single OSD staff office to have responsibility for the implementation of actions carried out pursuant to this initiative.

2. The Defense Investigative Service and the Defense Contract Audit Agency should be directed to monitor compliance with the requirements of Sec C., above, and report their findings to the appropriate OSD staff element on a periodic basis.

3. An extensive education and awareness program, designed to convey the requirements of this initiative to DOD employees engaged in export licensing cases, patent application cases, public affairs review, and to such employees and contractors involved in affected programs, should be instituted immediately after the features of the program have been developed and approved.

4. Appropriate administrative measures should be taken to redress violations of the requirements imposed under this program.